[00041] The wireless telephone or personal digital assistant 106 may be designed in accordance with the wireless application protocol, or WAP, which is a simplified version of the hypertext transfer protocol, or HTTP, used by the browser 114 within the user's PC 110 to communicate over the Internet.

[00042] The WAP wireless telephone or PDA 106 communicates via a wireless link with a WAP proxy and gateway 116 having an operating system 118 and from the gateway 116 through a firewall 120 to the Internet 102. The user's PC 110 communicates over conventional telephone lines, over leased digital telephone lines, over a cable access television (CATV) or other broadband system to an independent service provider (ISP) proxy and gateway 122 and from there through a firewall 124 to the Internet 102. There may also be a radio link between the user's PC 110 and some form of a base station, which may contain a local router, such that the PC 110 may also be wireless and may even be portable.

[00043] When a user wishes to make a purchase from a vendor's web site 104, the user of a PC 110 browses through HTML or XML shopping pages reviewing descriptions of products and selecting those products. In the case of a wireless telephone or PDA 106, the user might typically browse through handheld device mark-up language (HDML) or wireless mark-up language (WML) pages in the same manner, using typically simplified, smaller pages. When the user is ready to make a purchase, the user clicks on (or touches with a stylus) a link to a "secure form" 126, asking that this form be displayed on the user's browser 108 or 114, so that the user may fill in the blanks is this form. The form solicits information such as name, address, credit card number, password (PIN, PKI certificate, etc.) and other such personal information that is needed to complete a purchase. There is an important difference between this link, which is a secure link, and an ordinary hypertext link. An ordinary link in a typical web page is prefixed by "HTTP://..." to indicate that a web page is to be downloaded using the hypertext transfer protocol in the case of the PC 110. However, a secure page has an address that is prefixed with "HTTPS://..." to indicate that the downloading is to be done in a secure manner from a secure web site, using encryption, public-private keys, and site validation by digital identification.

[00044] Modern user's browsers 108 and 114 and modern web sites 104 are designed to include secure socket layer (SSL) technology, which provides for an encrypted and secure two-way communication between a user and a vendor with such sensitive information. Companies such as VeriSign, Incorporated provide this software and also provide computational techniques whereby the integrity and identity of a given vendor's web site may be verified using a server's digital identification (I.D.) 128. The details of all this are well

known and need not be explained here in full detail. For communication from the WAP Gateway 116 to the User's Wireless Telephone or PDA 106, the secure transmission is switched from SSL to Wireless Transport Layer Security (WTLS). WTLS performs the same function as SSL but is used for encrypted communication over airwaves from a wireless device to a WAP gateway.

[00045] The user's browsers 114 and 108 process this type of link differently than they do a normal link. They initiate a connection with the vendor's web site 104. The server at the vendor's web site responds by sending back its digital I.D. 128 to the browser 108 or 114. Then software in the user's browser 108 or 114 verifies the server's digital I.D. to gain assurance that the name of the web site corresponds to the corporate vendor having that name and is not a fraudulent web site. The user's browser 114 or 108 then sends the vendor's server a session key encrypted using the public key of the vendor.

[00046] Once that step is completed, a secure communication dialog can begin between the browser 114 or 108 and the vendor's web site 104. As a first step in this secure communication dialog, the browser 114 or 108 request the downloading of a personal information form 126. This form is displayed to the user, who fills in the blanks, or open fields, in the form and then executes a command that returns all of the supplied information back to the vendor's web site 104 where the purchase transaction is then completed.

[00047] The present invention contemplates relieving the user of the necessity of having to manually complete such forms. Accordingly, as a first step towards this goal, the preferred embodiment of the present invention provides a data flow monitor 300a installed within the operating system 118 of the WAP proxy and/or gateway 116 that services the WAP wireless telephone or PDA 106. Likewise, the present invention provides within the operating system 112 of the user's PC 110 a similar data flow monitor 300b. Where there is a wireless device with an operating system (such as a mobile phone or a PDA) the data flow monitor can be installed within the operating system of the wireless device. The data flow monitors 300a and 300b are customized to the characteristics and protocols of the operating systems 112 and 118 within which they are embedded. The data flow monitor may also be partially reswident on the device (PC 110 or wireless telephone or P.D.A. 106) and partially on a server, such as the one containing the proxy and gateway 116 and 122 or on some other convenient server.

[00048] The reason why the data flow monitor 300a is installed as an "add on" within the proxy and gateway 116 while the data flow monitor 300b is installed as an applet within the operating system 112 of the PC 110 is that many wireless telephones and other

accessories do not truly have an operating system that could be modified by means of an applet and, accordingly, it is essential to install the data flow monitor at the proxy and gateway 116. In a hybrid system, a proxy and gateway may have some clients that have an operating system and that may contain a data flow monitor and other clients that have no operating system and no data flow monitor. In this case, a simple priority scheme causes the appropriate data flow monitor to be selected while the other is disabled for a particular client session with the proxy and gateway. And, as mentioned above, the data flow monitor 300 may be resident, in part, on some server.

[00049] In either case, the data flow monitor is a simple program installed within the TCP/IP stack that monitors the flow of data packets leaving the browsers 108 and 114 looking for those packets that contain a request for the downloading of a secure page. While there are many ways that such packets could be identified, one way would be, for example, to examine such packets at the TCP level to determine to which socket number in the vendor's web site 104 each packet is addressed. Normal requests for hypertext pages are addressed to socket number 80 within the server, while secure web page download requests are normally addressed to a different socket number.

[00050] When the data flow monitor 300a or 300b detects such a secure request for the downloading of a form, it intercepts the request and reroutes it to a form fill proxy 400a or 400b by changing the request's internal IP address from that of the vendor's web site 104 to that of the form fill proxy 400a or 400b. Accordingly, the form fill proxy 400a or 400b ends up receiving the secure access request, which contains the web address of the personal information form 126 on the vendor's web site 104.

[00051] After verifying the authenticity of the vendor's web site as well as the identity of the user, the form fill proxy 400a or 400b downloads the personal information form 126 from the vendor's web site 104 and passes it to the form fill system 200a or 200b to be filled out using personal information that is retrieved from a wallet database 1100, as will be explained below. The completed form is then returned to the form fill proxy 400a or 400b which normally causes the form to be displayed upon the user's browser 108 or 114 so that the user may review and correct the information in the completed form. The form is then returned to the form fill proxy 400a or 400b at the same time that it is submitted to the vendor's web site 104. The system operates to intercept the form going in both directions, coming from the merchant to the customer and coming back from the customer to the merchant. However, in cases where the form is well-known and the rules for completing the form automatically are settled and established, user feedback may not be necessary, and the